ESTUDIO DE LA SEGURIDAD DEL PROTOCOLO TPMS
VULNERABILITIES IN THE TPMS PROTOCOL

ALBERTO CABALLERO GÁMEZ

DEPARTAMENTO DE ARQUITECTURA DE COMPUTADORES Y AUTOMÁTICA
FACULTAD DE INFORMÁTICA
UNIVERSIDAD COMPLUTENSE DE MADRID

Trabajo Fin de Grado en Ingeniería de Computadores

Agosto 2020

Director/es y/o colaborador:

Juan Carlos Fabero Jiménez
José Luis Vázquez Poletti

Resumen

La seguridad vial constituye uno de los problemas sociales y económicos más importantes de nuestro tiempo. Los avances tecnológicos en el área de las telecomunicaciones y el diseño de distintos dispositivos electrónicos especializados contribuyen a prevenir los accidentes, ya que inciden de forma directa en la seguridad activa del vehículo.

Algunos de estos dispositivos de protección se han decretado obligatorios en la fabricación en serie de vehículos. De esta forma, sistemas como ABS (Anti-lock Braking System), Airbags frontales, ESP (Electronic Stability Program) y TPMS (Tire Pressure Monitoring System) ya vienen incorporados.

A la vez que la Unión Europea hizo obligatorio el ESP, la norma se completó con la incorporación de los sistemas TPMS. Este sistema proporciona información acerca del estado de los neumáticos y mediante señales de radio la envía al sistema central del vehículo, para en última instancia lanzar alertas sobre cambios de temperatura y presión.

En el aspecto de seguridad vial el sistema TPMS proporciona grandes beneficios, ya que es capaz de alertar de anomalías en los neumáticos, lo que contribuye a evitar posibles accidentes. Sin embargo, a pesar de sus indudables ventajas, es necesario tener en cuenta el aspecto de la seguridad desde un punto de vista tecnológico.

En el estudio que se llevará a cabo evaluaremos los riesgos de estos sensores, analizando cómo podría verse comprometida la seguridad ante un ataque de réplica de la señal o manipulación de la misma.

Palabras clave

- TPMS (Tire-pressure Monitoring System)
- SDR (Software Defined Radio)
- Modulaciones FSK (Frequency Shift Keying) y ASK (Amplitude Shift Keying)
- Codificaciones Mánchester
- Demodulación y descodificación de señales
- RTL_433
- Telecomunicación

Abstract

Road safety is one of the most important social and economic problems of our time. Technological advances in the area of telecommunications and the design of various specialized electronic devices help prevent accidents as they have a significant direct impact on active vehicle safety.

Some of these protection devices have been decreed mandatory in mass production of vehicles, thus systems such as ABS (Anti-lock Braking System), Front Airbags, ESP (Electronic Stability Program) and TPMS (Tirepressure Monitoring System) are already incorporated.

At the same time that the European Union made ESP mandatory, the standard was completed with the incorporation of TPMS systems. This system provides tire condition information. With radio signals it is able to send this information to the central system of the vehicle, this central system will throw alerts about possible changes of temperature and pressure.

In terms of road safety, the TPMS system provides great benefits as it is able to alert about anomalies at the tires, which contributes to avoid possible accidents. However, despite its undoubted advantages, it is necessary to take into account the aspect of security from a technological point of view.

In the study that will be carried out we will evaluate the risks of these sensors, analyzing how the safety can be compromised in the event of a attack by signal replication or manipulation of it.

Keywords

- TPMS (Tire-pressure Monitoring System)
- SDR (Software Defined Radio)
- FSK (Frequency Shift Keying) and ASK (Amplitude Shift Keying) modulations
- Manchester encodings
- Signal demodulation and decoding
- RTL_433
- Telecommunication

Índice general

Agradecimientos

En primer lugar quiero agradecer a los directores de este Trabajo de Fin de Grado, Juan Carlos Fabero Jiménez y José Luis Vázquez Poletti, por la oportunidad que me han otorgado al poder participar en este proyecto. En especial quiero destacar la implicación de Juan Carlos Fabero Jiménez sin la cual no me habría sido posible su realización.

Mencionar igualmente el apoyo y la ayuda brindada por familiares y amigos, los cuales desde el inicio del grado hasta su finalización han estado dispuestos a prestar ayuda ante cualquier situación, y sin los cuales no habría sido posible cumplir este objetivo tan importante para mi desarrollo personal y profesional.

Capítulo 1

Introducción

A través del tiempo han ido evolucionando los sistemas de comunicación, lo que sin duda ha sido muy beneficioso para la humanidad. Esta revolución tecnológica no está exenta de riesgos como son los ciberataques, por esta razón es necesario el análisis y la evaluación de los nuevos dispositivos que se incorporan a nuestras vidas.

En este capítulo se presentará uno de estos dispositivos, en concreto, el sistema TPMS. Este dispositivo junto con el uso de diferentes tecnologías será el objeto de estudio de este TFG.

1.1. Estado del arte

Desde la antigüedad hasta la época actual el ser humano ha tratado de comunicarse haciendo uso de diferentes técnicas ya fuesen acústicas o visuales, antiguamente se utilizaban medios como tambores, cuernos o almenaras y señales de humo.

En la actualidad se ha modernizado esta comunicación haciendo uso de señales micro-ondas, con la ventaja de obtener un mayor alcance y una transmisión más detallada de la información, pero manteniendo la idea primigenia.

El sector de la telecomunicación se encuentra presente en muchos ámbitos, surgiendo en primera instancia para solucionar los problemas de comunicación a larga distancia, que vienen derivados de la necesidad de una mayor organización ante el imparable crecimiento de las civilizaciones.

El área de las telecomunicaciones estudia, entre otros aspectos, la transmisión y recepción de señales de carácter electromagnético. Dentro del espectro electromagnético, una banda determinada podrá identificarse mediante la longitud de onda, frecuencia e intensidad de la onda. Por ejemplo, las señales microondas son ondas electromagnéticas comprendidas entre frecuencias de 300MHz y 300GHz.

La radiocomunicación consiste en la transmisión a corta o larga distancia de información, utilizando para ello sistemas electrónicos y tecnológicos. Para establecer una comunicación simple son necesarias dos estaciones o máquinas distribuidas equipadas con módulos de emisión/recepción. De esta forma se cumpliría el objetivo de habilitar la comunicación y el intercambio de mensajes entre ambas. Un ejemplo de esta comunicación simple esta reflejada en la figura 1.1.

Figura 1.1: Ejemplo de una telecomunicación entre dos estaciones, fuente: https://demulacion.blogspot.com/2019/05/comunicaciones-conmicroondas-radio.html

La comunicación entre máquinas nos permite llevar a cabo avances con el fin de facilitar las necesidades que se presentan en la vida cotidiana del ser humano. Estos avances desarrollan principalmente sistemas de comunicación como internet, televisión, radio o redes

móviles. La característica común de estos sistemas es que precisan de dispositivos capaces de emitir y recibir señales microondas. Un ejemplo de estos dispositivos son los módulos RF (Radio Frequency).

Mediante el uso de módulos RF y diferentes sensores, se pueden implementar sistemas capaces de transmitir y recibir información acerca del entorno en el que están ubicados. Por ejemplo, sistemas como estaciones meteorológicas domésticas que informan sobre la condiciones ambientales, o como se verá en este estudio, los sistemas TPMS que informan del estado de los neumáticos de un vehículo.

En términos de comunicación mediante señales de radio hay que destacar una concatenación de etapas necesarias, desde la construcción de la trama de datos que se desea transmitir hasta la recepción de la misma. Para poder llevar a cabo la trasmisión de datos el emisor y el receptor deben tratar la señal de la misma forma; así como si se tratase de la comunicación entre dos personas, el tratamiento de la señal sería el lenguaje.

Dentro del contexto de la generación de señales cabe destacar la diferencia entre los tipos de datos y señales. Existe una gran diversidad de datos que se pueden transmitir, desde una onda sonora de voz, hasta la transmisión de datos binarios que corresponden respectivamente a datos analógicos de carácter continuo y digitales de carácter discreto. Los dos tipos de datos pueden transmitirse a través de señales digitales o analógicas, y la elección del tipo de señal dependerá en gran medida del medio de transmisión. De esta forma, para una transmisión por radio generalmente se utilizarán señales analógicas y para transmitir por cable señales digitales.

Los datos digitales permiten la aplicación de algoritmos matemáticos para la detección y corrección de errores, lo que se traduce en una mayor fiabilidad de la información transmitida. La fiabilidad que proporcionan este tipo de datos hace que algunos medios como la televisión, que antes transportaba datos analógicos mediante señales analógicas, haya

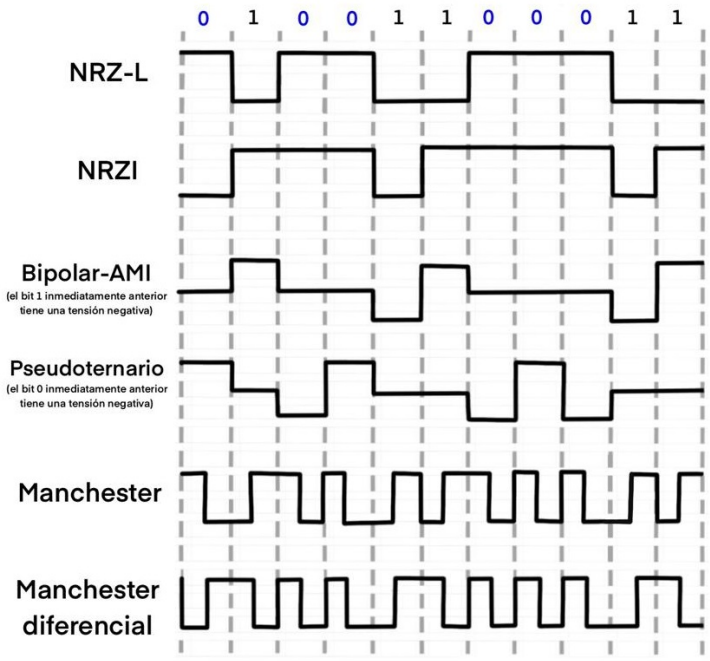
cambiado el tipo de datos que transmite al formato digital (TDT).

Las señales analógicas presentan un menor coste en cuanto a ancho de banda, aunque presentan desventajas como la complejidad de solucionar fallos de transmisión, la degradación del contenido tras replicar o amplificar la señal, y el volumen de datos que permiten transmitir. Sin embargo, hay algunos contextos en los que sí se siguen utilizando, como es el caso de la telefonía móvil.

Las señales digitales pese a su alto consumo de ancho de banda permiten el envío de un mayor volumen de datos, contando con la ventaja adicional de no producir deterioro en la información transmitida por mucho que la señal se amplifique o replique. Estas señales son las más utilizadas en comunicación, ya que para la transmisión de información a menudo es preferible que la señal sea eficiente más que económica.

En el caso de transmisión de datos digitales sobre señales digitales, algunas de las codificaciones más utilizadas se pueden observar en la figura 1.2.

Figura 1.2: Codificaciones digitales comúnmente utilizadas



La codificación de la señal es un proceso determinante para la transmisión de datos digitales. El resultado de la codificación se puede representar como una señal digital con tipo de onda discreta.

En el caso de la transmisión de señales analógicas y datos digitales, la señal debe modularse para poder transmitirse. Las diferentes técnicas de modulación se pueden clasificar según los datos que se pretenden transmitir.

Los datos analógicos se modulan mediante las técnicas FM (Frequency Modulation) y AM (Amplitude Modulation), que análogamente corresponden a ASK (Amplitude Shift keying) y FSK (Frequency Shift Keying) si se tratase de datos digitales. Estas técnicas se aplican alterando las características de la onda portadora.

$$\lambda = \frac{c}{f}$$

Haciendo especial inciso sobre las técnicas para transmitir datos digitales por un medio analógico se podrían diferenciar las siguientes modulaciones digitales:

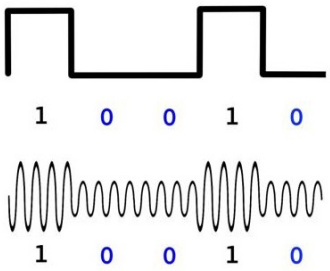
- Modulación ASK (Amplitude Shift keying)

  Si se modifica la amplitud de la onda portadora y se asigna una amplitud diferente para cada símbolo se obtiene la modulación ASK.

  $$s(t) = A_0 * \sin(2\pi f t + \theta) \text{ bit} = 0$$
  $$s(t) = A_1 * \sin(2\pi f t + \theta) \text{ bit} = 1$$

  En el caso de ASK con un índice de modulación inferior al 100 % surgirá una forma de onda como se representa en la figura 1.3.

Figura 1.3: Ejemplo de modulación ASK



- Modulación OOK (On-Off Keying)

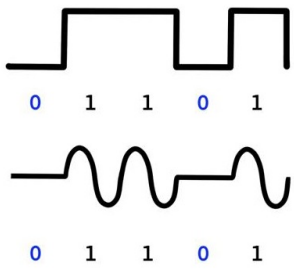
  De forma idéntica a ASK, la modulación OOK altera la onda modificando los valores de la amplitud.

  La modulación OOK tiene la particularidad de tener un índice de modulación del 100 %. El resultado que genera es una forma de onda donde la amplitud para el símbolo 0 sería nula. El aspecto de una señal modulada mediante OOK está reflejada en la figura 1.4.

$$s(t) = (0) * \sin(2\pi f t + \theta) \text{ bit} = 0$$

$$s(t) = A_1 * \sin(2\pi f t + \theta) \text{ bit} = 1$$

Figura 1.4: Ejemplo de modulación OOK



- Modulación PSK (Phase Shift Keying)

  Es una modulación angular cuya señal moduladora es digital, con un número de estados limitado. Esta es la principal diferencia con la modulación analógica PM (Phase

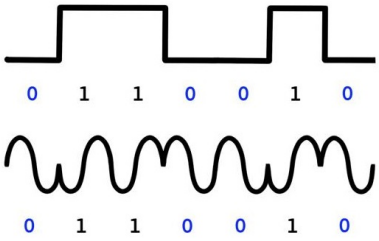
Modulation) en la que la señal moduladora es continua.

Al modificar la fase de la onda portadora y asignando un desplazamiento de fase diferente para cada uno de los símbolos se obtiene un aspecto de onda como el representado en la figura 1.5.

$$s(t) = A * \sin(2\pi ft + \theta_0) \text{ bit} = 0$$

$$s(t) = A * \sin(2\pi ft + \theta_1) \text{ bit} = 1$$

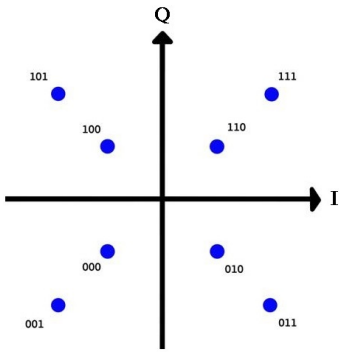
Figura 1.5: Ejemplo de modulación PSK



- Modulación QAM (Quadrature Amplitude Modulation)

  Si se manipula la amplitud y la fase de manera simultánea se obtiene como resultado una modulación QAM. El diagrama de constelación generado por esta modulación se observa en la figura 1.6.

Figura 1.6: Diagrama de constelación de modulación 8-QAM



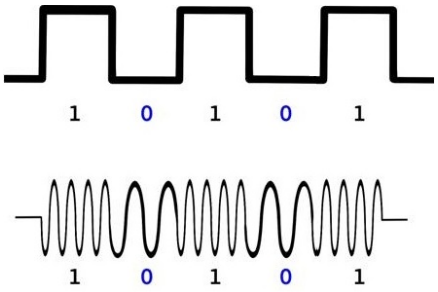
- Modulación FSK (Frequency Shift Keying)

  En el caso de la modulación FSK cada símbolo es expresado con una frecuencia diferente, lo que permite generar una onda como la representada en la figura 1.7.

$$s(t) = A * \sin(2\pi f_0 t + \theta) \text{ bit} = 0$$

$$s(t) = A * \sin(2\pi f_1 t + \theta) \text{ bit} = 1$$

Figura 1.7: Ejemplo de modulación FSK



1.2. Sistema TPMS

El sistema TPMS ha pasado a ser elemento obligatorio desde hace relativamente poco, siendo necesaria la inclusión de este en los vehículos actuales.

Este sistema, con la función de informar en todo momento al conductor sobre el estado de los neumáticos, es parte de la seguridad activa de los vehículos modernos, y para llevar a cabo su función hace uso de diferentes tecnologías. Según las características de la tecnología que utilizan se pueden diferenciar dos tipos de sistemas TPMS:

- TPMS indirecto:

  Los vehículos cuentan con diversas tecnologías, entre ellas se encuentra el sistema ABS que hace uso de un sensor de revoluciones en cada rueda para monitorizar un posible bloqueo de los neumáticos.

Si se tiene en cuenta que la presión del neumático repercute de forma directa sobre su diámetro, si disponemos de una rueda que se encuentre en estado de pérdida de presión, ésta necesitará de un mayor número de revoluciones que el resto para recorrer la misma distancia. De esta forma, el sistema TPMS de medición indirecta con ayuda del sensor de revoluciones de ABS concluye que, si una rueda gira a mayor velocidad en comparación con el resto, el neumático estará sufriendo una pérdida de presión lo que provocará que envíe una señal de alarma al sistema central o ECU (Engine Control Unit) del vehículo, el cual informará mediante señales acústicas y/o visuales al conductor.

- TPMS directo:

  El sistema TPMS directo tiene el mismo objetivo que el sistema de medición indirecta, con la diferencia de disponer de sensores de presión y temperatura integrados. Este dispositivo se suele situar en el interior del neumático donde los sensores pueden llevar a cabo las mediciones correspondientes.

  La comunicación con la ECU se lleva a cabo mediante el envío de datos digitales, utilizando para ello la modulación/codificación especificada por cada fabricante.

En términos de comunicación el protocolo TPMS utiliza microondas para poder informar a la mencionada ECU del vehículo. Para ello emite una señal de radiofrecuencia comprendida en el rango [315MHz – 440MHz] dependiendo de la región en la que se encuentre.

La banda de frecuencia 433MHz es la utilizada para la intercomunicación de dispositivos de baja potencia en territorio europeo, por esta razón será la frecuencia sobre la que se actuará en este estudio sobre el protocolo TPMS.

1.3. Objetivos del trabajo

El objetivo principal de este TFG es llevar a cabo el estudio y el análisis de seguridad del protocolo TPMS, cuya implementación es obligatoria en los vehículos actuales.

Para ello se procederá a realizar un análisis de las señales captadas en la banda 433MHz mediante la utilización de un dispositivo especializado en la recepción de señales de radio (Dongle RTL-SDR), y el uso de *software* libre para descodificar la señal recibida.

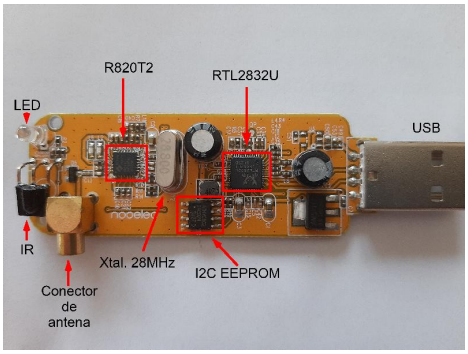
Así, el objetivo final del trabajo consistirá en evaluar la dificultad y el coste de realizar un ataque de réplica de señal al tiempo que es posible manipular la información enviada.

1.4. Tecnologías utilizadas

- Dongle RTL_SDR

  Es un dispositivo que funciona como receptor de radiofrecuencia. Este dispositivo mediante el uso de una antena recibe la señal y con ayuda de *software* permite obtener la demodulación y descodificación de la misma. El objetivo de utilizar este dispositivo es poder llevar a cabo el análisis del espectro y estudiar las características de las señales recibidas.

Figura 1.8: Interior de un USB rtl_sdr



- RTL_433

  El RTL_433 [5] es un *software* de código abierto que permite la decodificación de tramas de dispositivos en las bandas de frecuencia de 433MHz. Entre estos dispositivos se encuentran algunos de los sistemas TPMS utilizados por los vehículos modernos. Este *software* facilita tareas como entender el formato de la trama de la señal y llevar a cabo las pruebas necesarias para comprobar la señal que se pretende generar.

  Mediante el uso de dispositivos diseñados con el propósito de emitir señales de radio se puede llevar a cabo una réplica de la señal de manera sencilla pues, como veremos, las señales del sistema TPMS se emiten sin cifrar.

- GNU-Radio

  Gnu-Radio proporciona un kit de herramientas de desarrollo para generar una señal modulada tras alimentar al diagrama de bloques implementado con un archivo de formato binario, el cual contendrá la información a transmitir por el emisor.

- Matlab

  Mediante el uso de Matlab realizaremos la construcción de la trama para un dispositivo específico, siendo necesaria la implementación de código que permita la codificación de la trama y la generación de un archivo en formato binario para poder ser modulada posteriormente por GNU-Radio.

- Dispositivo TPMS

  Se dispondrá de dispositivos TPMS para llevar a cabo el estudio de la señal y entender el espectro frecuencia que forman.

Figura 1.9: Ejemplo de un dispositivo TPMS oficial, fuente: Juan Carlos Fabero Jiménez

Capítulo 2

Introduction

Through time communication systems have evolved, which has undoubtedly been very beneficial for humanity. This technological revolution is not without risks such as cyberattacks, for this reason it is necessary to analyze and evaluate the new devices that are incorporated into our lives.

In this chapter will be introduced one of these devices, specifically, the TPMS system. This device together with the use of different technologies will be the object of study of this TFG.

2.1. State of the art

From ancient times to the present time, human beings have tried to communicate using different techniques whether acoustic or visual, in the past media such as drums, horns or beacons and smoke signals were used.

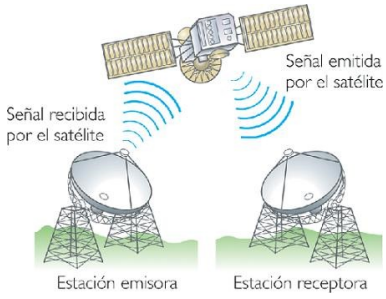
At present, this communication has been modernized by making use of microwave signals, with the advantage of obtaining a greater range and a more detailed transmission of information, while maintaining the original idea.

The sector of telecommunications is found in many ambit, arising in first instance to provide solutions of long way communications derived of the needs of a greater organization before the unstoppable growth of the civilizations.

The telecommunications area is in charge of studying among other aspects the transmission and reception of electromagnetic signals. Inside the electromagnetic spectre one band can be identified through the length of the wave, frequency and intensity of the wave. For example, the microwave signals are electromagnetic waves between the 300MHz and 300GHz frequencies.

The radio-communication consist in long or short distance transmission of information, using for that electronic and technological systems. To establish a simple communication is necessary two stations or distributed machines equipped with emission/reception modules. In this way it the objetive of enable communication and the exchange of messages between both machines would be fulfilled. An example of this simple communication is reflected in figure 2.1.

Figura 2.1: Telecommunication example between two stations, source: https://demulacion.blogspot.com/2019/05/comunicaciones-conmicroondas-radio.html



The communication between machines allows us to carry out advances in order to solve some of the problems of human daily life. This advances mainly develops communication systems as internet, television, radio or mobile networks. The common characteristic of these systems is that they require devices capable of emitting and receiving microwave signals. An example of these devices are RF (Radio Frequency) modules.

Through the use of RF modules and different sensors, systems capable of transmitting and receiving information about the environment in which they are located can be implemented, for example, systems such as domestic weather stations that report on environmental conditions, or as it will be seen in this study, the TPMS systems that report about the condition of a vehicle's tires.

In terms of communication through radio signals, a concatenation of necessary stages must be highlighted, from the construction of the data frame that we want to transmit to its reception. In order to carry out the data transmission, the sender and the receiver must treat the signal in the same way. As if it was communication between two people, the signal treatment would be language.

Within the context of signal generation it is worth highlighting the difference between the types of data and signals. There is a great diversity of data that can be transmitted, from the sound wave of a voice to the transmission of binary data type that correspond respectively to analogical data of continuous character and digital data of discrete character. The two type of data can be transmitted through digital or analogical signals, and the election of the tipe od signal will depend largely of the transmision medium. In this way, analog signals will generally be used for radio transmission and digital signals for cable transmission.

Digital data allows the application of mathematical algorithms to detect and correct errors, which means greater reliability of the information transmitted. The reliability provided by this type of data makes some media such as Television, which previously carried analog data using analog signals, has changed the type of data it transmits to digital format (DTT).

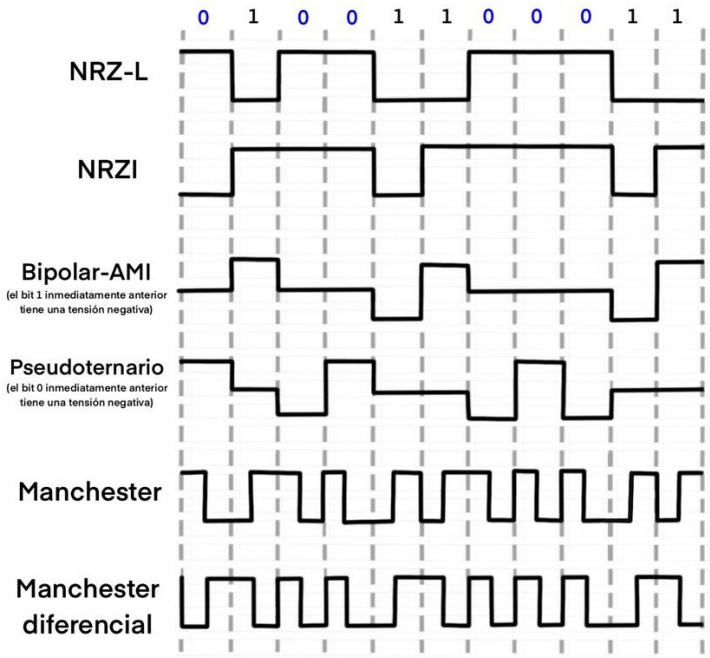
The analogical signals present a lower cost at the bandwidth, although they present disadvantages like the complexity to solve transmission problems, the degradation of the content after replicate or amplify the signal, and the data volume that are able to transmit.

However, there are some context that are still on use, like is the case of mobile communications.

The digital signals despite their high consume of bandwidth allow to send a higher volume of data, with the additional advantage of not causing deterioration in the information transmitted no matter how much the signal is amplified or replicated. This signals are the most used in communication, since for the transmission of information it is often preferable that the signal be efficient rather than economic.

In the case of digital data transmission over digital signals, some of the most commonly encodings can be seen in the figure 2.2.

Figura 2.2: Digital encodings commonly used



Signal encoding is a determinant process for the transmission of digital data. The result of this codification can be represented by a digital signal with discrete-wave type.

In the case of transmission of analog signals and digital data, the signal must be mo-

dulated before it can be transmitted. The different modulation techniques can be classified according to the data prented to transmitt.

The analogical data are modulated though FM (Frequency Modulation) and AM (Amplitude Modulation), that similarly correspond to ASK (Amplitude Shift keying) and FSK (Frequency Shift Keying) if the data were digital. This techniques are applied by alteration the characteristics of the carrier wave.

$$\lambda = \frac{c}{f}$$

Making a special attention to the techniques to transmit digital data through an analogical medium the following digital modulations could be differentiated:

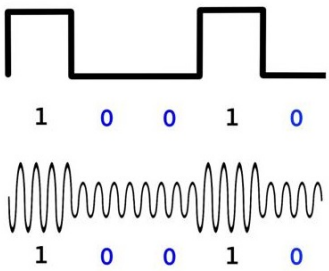
- ASK (Amplitude Shift keying)

  Modifying the amplitude of the carrier wave and assigning a different amplitude for each symbol is obtained the ASK modulation.

$$s(t) = A_0 * \sin(2\pi f t + \theta) \text{ bit} = 0$$
$$s(t) = A_1 * \sin(2\pi f t + \theta) \text{ bit} = 1$$

  In the case of ASK with a modulation index lower than 100 % a waveform with the characteristics reflected at the figure 2.3 will appear.

Figura 2.3: ASK modulation example



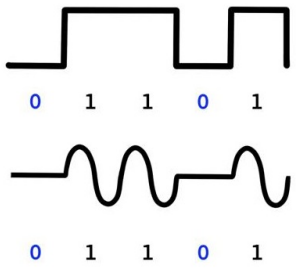
- OOK (On-Off Keying)

  In the same way as ASK, OOK modulation alters the wave by modifying the amplitude values.

  The OOK modulation has the particularity of having a modulation index of 100 %. The result a waveform where the amplitude for the 0 symbol would be zero. The appearance of a signal modulated by OOK is reflected at the figure 2.4.

$$s(t) = (0) * \sin(2\pi f t + \theta) \text{ bit} = 0$$
$$s(t) = A_1 * \sin(2\pi f t + \theta) \text{ bit} = 1$$

Figura 2.4: OOK modulation example



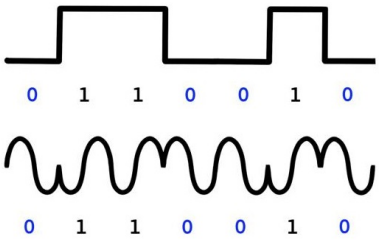
- PSK (Phase Shift Keying)

  It is an angular modulation whose modulating signal is digital, with a limited number of states. This is the main difference from PM analog modulation (Phase Modulation) in which the modulating signal is continuous.

  Modifying the phase of the carrier wave and assigning a different phase shift for each one of the symbols is obtained a wave aspect like the represented at the figure 2.5.

$$s(t) = A * \sin(2\pi f t + \theta_0) \text{ bit} = 0$$
$$s(t) = A * \sin(2\pi f t + \theta_1) \text{ bit} = 1$$

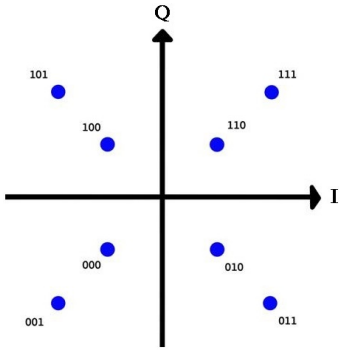
Figura 2.5: PSK modulation example



- QAM (Quadrature Amplitude Modulation)

  If the amplitude and the phase are simultaneously manipulated is obtained a QAM modulation as a result.The constellation diagram generated by this modulation is observed in the figure 2.6.

Figura 2.6: Constellation diagram of 8-QAM Modulation



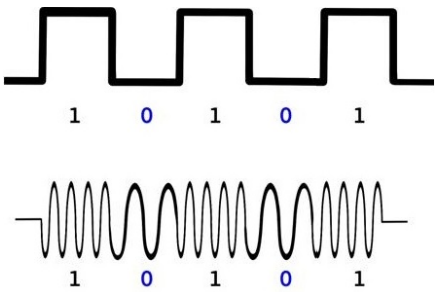
- FSK (Frequency Shift Keying)

  In the case of FSK modulation each symbol is expressed with a different frequency, allowing to generate a wave like the represented at the figure 2.7.

$$s(t) = A * \sin(2\pi f_0 t + \theta) \text{ bit} = 0$$

$$s(t) = A * \sin(2\pi f_1 t + \theta) \text{ bit} = 1$$

Figura 2.7: FSK modulation example



2.2. TPMS system

The TPMS system has become a mandatory element relatively recently, being necessary to include it in current vehicles.

This system, with the function of informing the driver about the condition of the tires at all times, is part of the active safety of modern vehicles, and to carry out its function it makes use of different technologies. Depending on the characteristics of the technology they use, two types of TPMS systems can be differentiated:

- Indirect TPMS:

  The vehicles count with different technologies, among them is included the ABS system which uses a revolution sensor on each wheel to monitor a possible blockage of the tires.

  Taking into account that the tire pressure has a direct effect on its diameter, if we have a wheel that is in a loss of pressure state, this will need a higher number of revolutions than the rest to travel the same distance. In this way the indirect measurement TPMS system with the help of the ABS revolution sensor concludes that, if a wheel rotates at a higher speed compared to the rest, the system will be suffering a loss of pressure sending an alarm signal to the central system or ECU (Engine Control Unit) of the vehicle, witch will inform with acoustic and/or visual signals the driver.

- Direct TPMS:

  The direct TPMS system has the same objective as the system of indirect measurement, with the difference of dispose about pressure and temperature sensors integrated. This device is usually located inside the tire where the sensors can carry out the correspondent measures.

  Communication with the ECU is carried out by sending digital data, using the modulation/encoding specified by each manufacturer.

In terms of communication the TPMS protocol uses microwaves to be able of inform the the mentioned ECU of the vehicle. In order to do that emits a radio frequency signal in the range [315MHz – 440MHz] depending on the region it's in.

The 433MHz frequency band is the used for the intercommunication of low power devices in European territory, for this reason it will be the frequency on which it will act in this study about the TPMS protocol.

2.3. Project Goals

The main goal of this TFG is to carry out the study and the analysis of the TPMS protocol safety, whose implementation is mandatory in current vehicles.

For this, an analysis of the signals captured in the 433MHz band will be carried out, by the use of an specialized device for the reception of radiosignals (Dongle RTL-SDR) and the use of free software to decode the received signal.

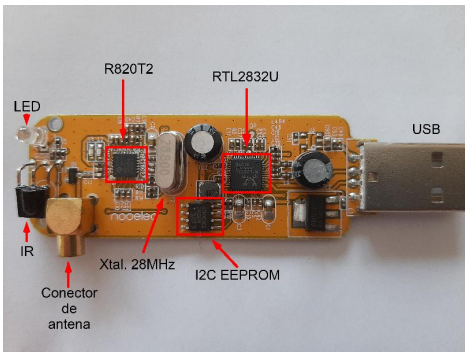
Thus, the final objective of the work will be to evaluate the difficulty and cost of carrying out a signal replication attack at the same time it is possible to manipulate the information sent.

2.4. Technologies Used

- RTL_SDR Dongle

  It is a device that works as a radio frequency receiver. This device by the use of a antenna receives the signal and with the help of software allows to obtain the demodulation and decoding of it. The objetive of using this device is to carry out the spectrum analysis and study the characteristics of the received signals.

Figura 2.8: The inside of a USB rtl_sdr



- RTL_433

  The RTL_433 [5] is an open source software that allows the decoding of device frames in 433MHz frequency bands. Among these devices are some of the TPMS systems used by modern vehicles. This software facilitates tasks such as understanding the frame format of the signal and carrying out necessary tests to verify the signal that is pretended to generate.

  By using devices designed for the purpose of emitting radio signals, and attack of signal replication can be carried out easily because, as we will see, the signals from the TPMS system are emitted without encryption.

- GNU-Radio

  Gnu-Radio provides a development toolkit that will allow us to generate the modulated

signal after feeding the implemented block diagram with a binary format file, wich will contain the information to be transmitted.

- Matlab

  Through the use of Matlab we will perform the construction of the frame for a specific device, being necessary the implementation of code that allows the coding of the frame and the generation of a file in binary format to be able to be modulated later by GNU-Radio.

- TPMS device

  A TPMS device will be available to carry out the study of the signal and understand the frequency spectrum they form.

Figura 2.9: Example of official TPMS device of a vehicle, source: Juan Carlos Fabero Jiménez

Capítulo 3

Análisis de espectros de radiofrecuencia

En este capítulo se verá cómo con el uso de un USB SDR y software específico se puede llevar a cabo la obtención de símbolos pertenecientes a datos digitales, que son transmitidos de forma analógica en las bandas de frecuencia de 433MHz.

3.1. Dispositivo USB RTL_SDR

La tecnología SDR (Software Defined Radio) es un sistema de radiocomunicación con la particularidad de que componentes normalmente implementados mediante *hardware*, como son moduladores, demoduladores o filtros, son implementados en software.

En marzo de 2010 Eric Fly [3] comenzó a investigar la captura de los paquetes USB del software de Windows en el modo FM/DAB. Lo que pretendía adquirir era un equivalente para Linux, y fue entonces cuando se pudo vislumbrar el potencial de la tecnología SDR.

Las posibilidades de esta tecnología provocaron el desarrollo de software especializado con el objetivo de aumentar y afianzar las funcionalidades del dispositivo. Como consecuencia del trabajo de compañías como Realtek [8] y Osmocom [6] el dispositivo fue dotado de la capacidad de sintonizar frecuencias desde los 24MHz. Desde entonces se han implementado

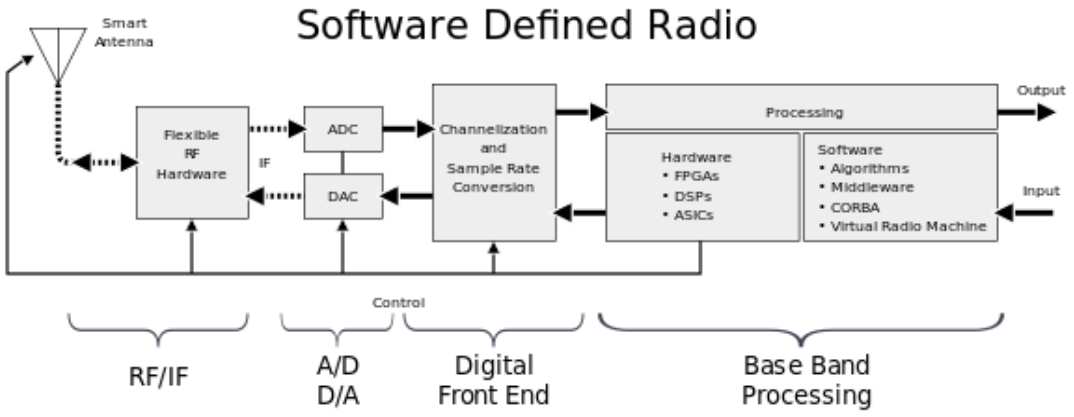
multitud de aplicaciones software con el objetivo de aprovechar las diferentes funcionalidades del SDR, entre las cuales nos podemos encontrar GQRX, SDR# y Gr-Air-Modes.

El *dongle* RTL_SDR nos habilita la recepción de señales comprendidas en el rango de 24MHz y 1GHz. Aunque no es el dispositivo idóneo debido a su baja sensibilidad y la necesidad de una antena con mejores características, sí permite la recepción de emisoras de radio FM comerciales.

Este dispositivo está basado en el chip Realtek RTL2832U [9] que con ayuda de un sintonizador actúa como demodulador de señales. Originalmente fue diseñado con el objetivo de dotar a los usuarios la posibilidad de sintonizar canales de televisión desde cualquier ordenador, recibiendo señales TDT/DVB-T y de radio digital DAB/DAB+. Actualmente es utilizado para una gran variedad de propósitos, como sintonizar bandas de frecuencia de radioaficionados, bandas aéreas o en este caso concreto, sintonizar las bandas de frecuencia a 433MHz para la recepción y análisis de las señales transmitidas por los sistemas TPMS.

El interior del dispositivo se encuentra representado de forma física en la figura 1.8. Si se simplifica el concepto, el diagrama de bloques de este dispositivo podría representarse como se muestra en la figura 3.1.

Figura 3.1: Diagrama de bloques conceptual de un transceptor SDR ideal, fuente: https://en.wikipedia.org/wiki/Software-defined_radio



La figura 3.1 muestra la idea conceptual de un transceptor SDR ideal. Como se observa, el objetivo consiste en conectar una antena a un conversor analógico digital. Este concepto no puede llevarse a cabo debido a las limitaciones tecnológicas derivadas de las grandes demandas del tiempo real, que se producen por las conversiones analógico-digitales y a la precisión requerida por el dispositivo.

El chip RTL2832U es un demodulador integrado con un ADC (Analog-to-Digital Converter) que cumple en cierto modo con las expectativas de recepción del transceptor SDR ideal. Este integrado, para realizar su función, utiliza un sintetizador basado en un PLL (Phase Locked Loop) con el objetivo de obtener un conjunto discreto de frecuencias de la señal recibida. El sintetizador hace de oscilador para un mezclador en cuadratura que produce como salida una banda base en el plano complejo, cuyo ancho de banda estará comprendido entre -BW/2 y BW/2. Esta información será muestreada mediante el ADC produciendo finalmente las muestras complejas (In-phase and Quadrature).

El R820T es un sintonizador de bajo consumo pero con alto rendimiento. Está compuesto por un PLL, un mezclador, un regulador de voltaje y un filtro de seguimiento; y realiza la función de un amplificador de bajo ruido. Este sintonizador permite su configuración a través de un bus I^2C y una memoria EEPROM.

Para la recepción y demodulación de señales se hará uso de uno de estos dispositivos RTL-SDR. El *hardware* del mismo consiste en una antena para recibir las señales analógicas, un sintonizador de radio (R820T2), para convertir la señal a una frecuencia menor intermedia IF (Intermediate Frequency) y por último un demodulador de señal que enviará los datos digitales a través del puerto USB al ordenador. Todo ello, junto al uso de software específico, facilitará la tarea de obtener las diferentes tramas de datos TPMS.

3.2. Inspectrum como analizador de señales

Inspectrum [10] es un software que permite analizar las diferentes señales permitiendo una demodulación de datos a través del espectro de la señal recibida. Para poder alimentar este programa en primera instancia hay que capturar la señal mediante el uso de software como GQRX, URH (Universal Radio Hacker) o RTL_433. Para comprobar el aspecto del espectro que emiten los dispositivos se utilizará GQRX.

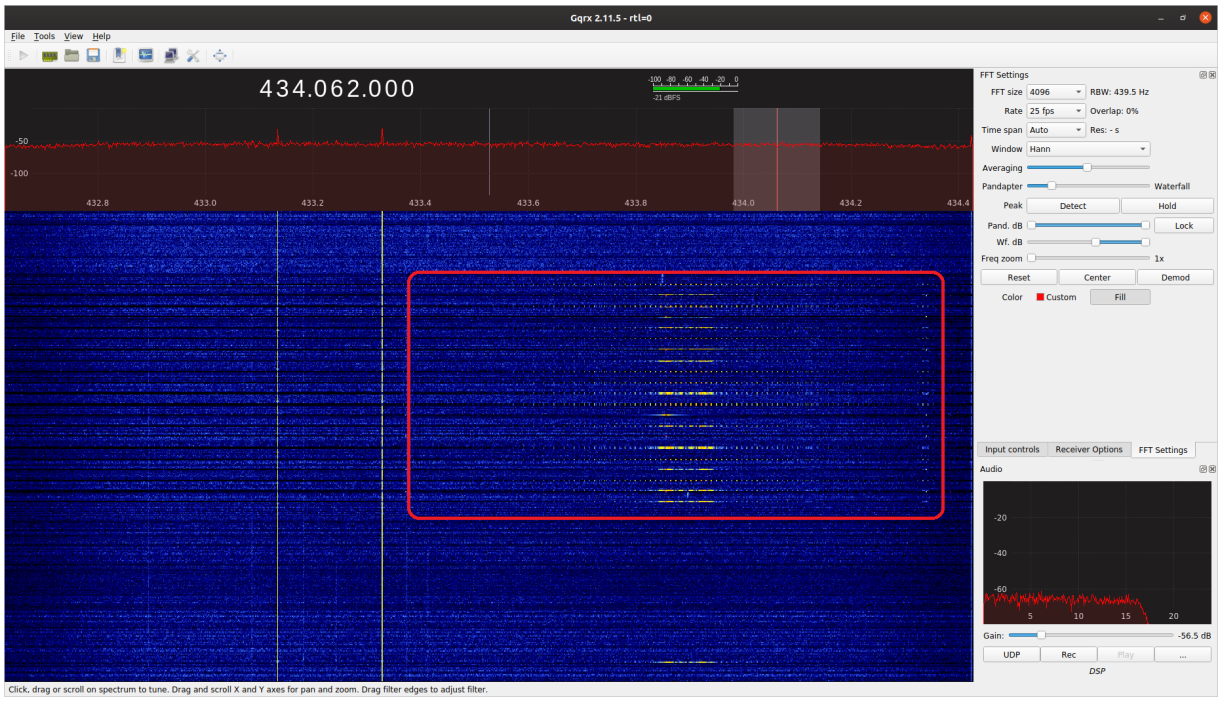
Las siguientes pruebas consistirán en el uso de un sistema TPMS no oficial[1] y una rueda de bicicleta para simular pérdidas de presión de manera sencilla, esto se debe a que el sistema TPMS utilizado sólo transmite en el caso de que ocurra esta situación. El montaje para llevar a cabo estas pruebas se puede observar en la imagen 3.2.

Figura 3.2: Montaje para la medición de sistemas TPMS

[1]Sistema TPMS adquirido en Amazon por un precio reducido y que no es utilizado por los distribuidores de vehículos oficiales.

En la figura 3.3 se puede observar cómo si sintonizamos la frecuencia central en el rango [433MHz – 434MHz] mediante GQRX, se obtiene el espectro de la señal producida por uno de estos sensores TPMS.

Figura 3.3: Señal transmitida por un dispositivo TPMS



Esta herramienta, GQRX, fue desarrollada con el fin de facilitar la escucha de diferentes bandas de frecuencia para observar y grabar comunicaciones de voz como puede ser el caso de radioaficionados, emisoras FM comerciales, comunicaciones en la banda aérea o incluso, en nuestro caso, el sonido característico transmitido por los dispositivos TPMS.

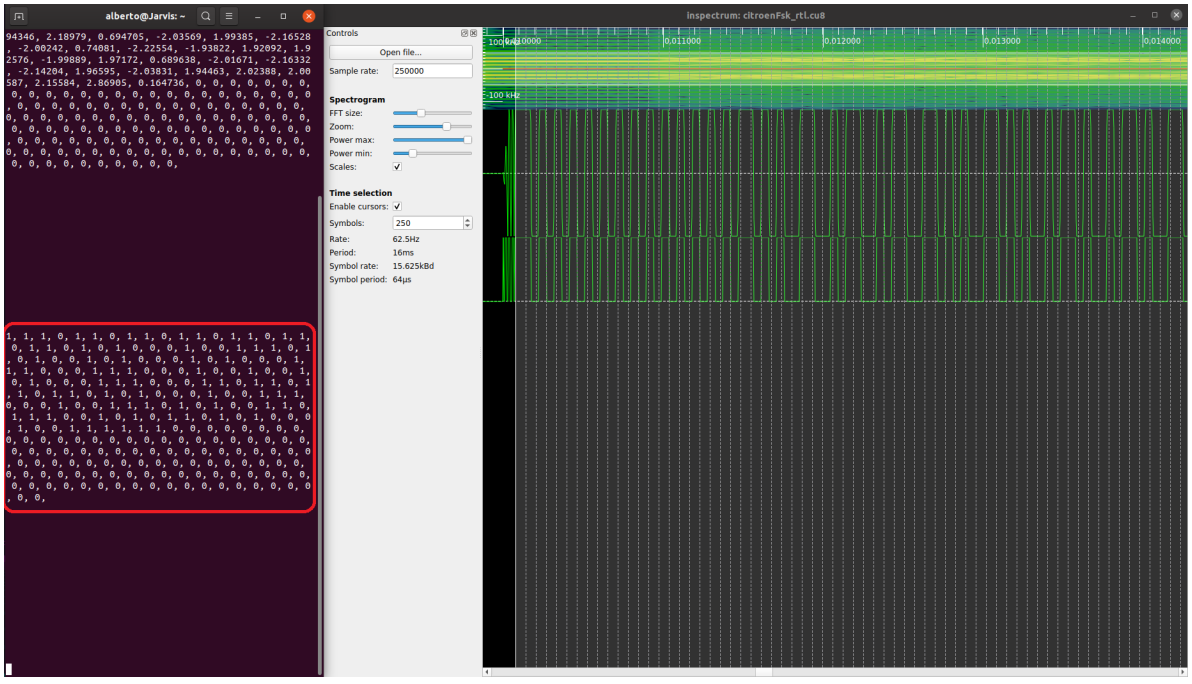
Por esta razón, el uso de este software es insuficiente para poder llevar a cabo un análisis exhaustivo de la señal transmitida por los dispositivos TPMS. Nuestro objetivo es poder obtener un flujo de bits y a partir de él, extraer de cierta forma el formato de la trama para el dispositivo concreto. Sin embargo, este software no proporciona por sí solo utilidades en cuanto a la transformación de la señal analógica en una señal con forma de onda cuadrada y mucho menos la obtención de símbolos.

Capturando la señal con alguna de las aplicaciones enumeradas anteriormente y en este caso concreto mediante el uso del *software* RTL_433, se podrá generar un archivo binario que se utilizará para alimentar al software Inspectrum, el cual permite analizar la señal de forma eficaz.

Este programa, dada una señal recibida en formato IQ (In-phase and Quadrature), permite mediante la selección del modo de demodulación ya sea FSK, ASK o PSK, generar una gráfica con la forma de onda cuadrada correspondiente.

Una vez obtenida esta onda cuadrada, Inspectrum permite la selección del ancho de símbolo, así como especificar el número de símbolos que se encuentran dentro de la señal. El siguiente paso consiste en exportar los símbolos ya sea a un archivo o por consola. Un ejemplo de ejecución de este proceso obteniendo como salida los símbolos binarios por consola queda reflejado en la figura 3.4.

Figura 3.4: Ejemplo de ejecución con Inspectrum



3.3. Uso del software RTL_433

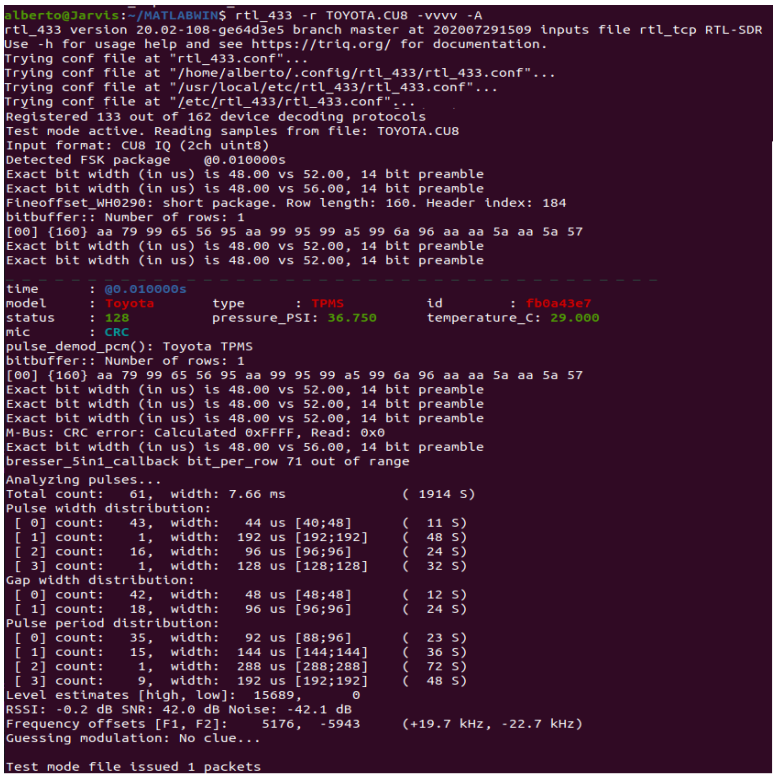
Como se ha observado mediante el uso de Inspectrum, mediante diferentes técnicas se puede llevar a cabo la obtención del formato de la trama para cada dispositivo TPMS. Sin embargo, es un proceso laborioso y complejo debido en gran parte a la falta de documentación en cuanto al formato de trama enviada por algunos dispositivos. Un ejemplo es el sistema TPMS no oficial para el que se realizaron las pruebas descritas en el apartado 3.2. No conocer la modulación, la codificación y el formato de la trama dificultó enormemente el análisis que se iba a llevar a cabo.

El *software* RTL_433 fue implementado por Benjamin Larsson [5] y actualmente existe una gran comunidad que trabaja conjuntamente para mantenerlo actualizado. Este software permite agilizar y simplificar el proceso para obtener el formato de trama, la demodulación y la decodificación de señales TPMS.

Este *software* no ofrece soporte para el sistema TPMS no oficial. Sin embargo, da soporte a una gran cantidad de dispositivos de carácter oficial. Dentro de los dispositivos que recoge se pueden encontrar los sistemas TPMS utilizados por marcas de vehículos populares como Citroën, Toyota, Ford, Renault, etc. Este *software* no sólo da soporte a los dispositivos TPMS, también admite dispositivos específicos de estaciones meteorológicas o del ámbito de la domótica. Además, permite añadir nuevos protocolos de manera relativamente sencilla, si se conocen los parámetros básicos de éstos, como la modulación, la codificación, el formato de la trama, etc.

RTL_433 produce como salida por consola los datos concretos de los dispositivos que emiten en la frecuencia 433MHz. Mediante el uso de las diferentes herramientas que proporciona permite obtener datos técnicos sobre la señal recibida. En la figura 3.5 se observa cómo mediante las opciones -vvvv y -A se obtienen datos como la modulación utilizada, el ancho de bit o información sobre el pulso.

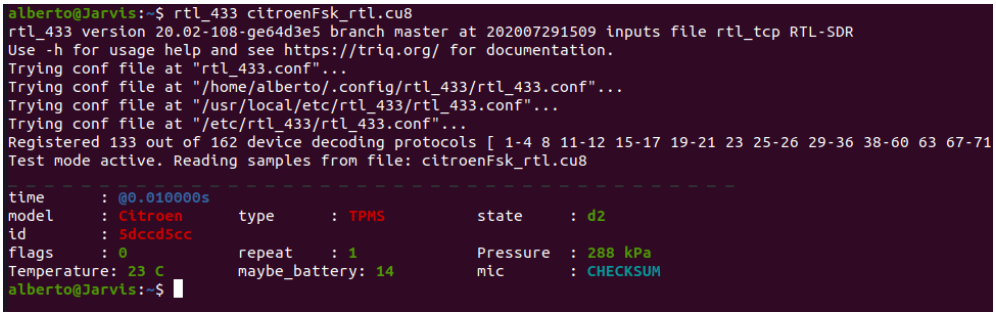
Figura 3.5: Datos técnicos sobre la señal emitida por un sistema TPMS Toyota



El código de esta aplicación es software libre, lo que permite navegar a través del mismo obteniendo datos concretos de gran interés. Gracias a esto se puede avanzar al siguiente paso y generar una señal adecuada para un dispositivo concreto.

En la figura 3.6 se observan los datos obtenidos por el programa RTL_433. En este caso se ignora la información detallada de la señal y se obtienen los datos relevantes para la ECU.

Figura 3.6: Trama Citroën obtenida mediante el *software* RTL_433



La imagen representa la trama de un dispositivo Citroën que informa sobre la presión y temperatura de los neumáticos, así como del estado de batería del dispositivo TPMS. En el caso de que cualquiera de estos valores se viese comprometido, la ECU será la encargada de enviar la señal de alerta correspondiente.

Capítulo 4

Generación de señales de radiofrecuencia TPMS

En este capítulo se verá cómo llevar a cabo la construcción de la trama para los dispositivos TPMS. Para conseguir dicha construcción se utilizará como base el *software* RTL_433, donde se encuentran detalles como los campos transmitidos en la trama de datos, los bits necesarios para cada campo, la modulación y codificación de los dispositivos TPMS de distribuidores oficiales.

4.1. Construcción de la señal TPMS

Dentro del contexto de las señales producidas por los dispositivos TPMS cabe destacar tres grandes aspectos que incidirán de forma directa en su generación.

En primer lugar, la construcción de la trama de datos que se estudiará en el apartado 4.2. En este proceso es necesario especificar la información que se desea transmitir, asignando los bits necesarios para cada campo.

El siguiente paso es la codificación de la trama de datos que se podrá ver en el apartado 4.3. El objetivo de codificar la señal es provocar transiciones que permitan la sincronía de

reloj o sincronía de bit, además de minimizar los errores múltiples de transmisión, mediante el uso de códigos Gray.

Por último, se procederá a la generación de la señal mediante la modulación, cuyo proceso se verá en el apartado 4.4. Como se ha explicado en capítulos anteriores, la modulación de los datos digitales permite el envío de información a través de un medio analógico.

4.2. Estructura de la trama de datos

La trama adecuada para estos dispositivos deberá tener un aspecto similar al reflejado en la figura 4.1. Esta trama es orientativa, ya que dependiendo del fabricante se podrán incluir más campos en el envío.

Figura 4.1: Formato simplificado de una trama TPMS

En el artículo Design of Direct-Type Tire-Pressure Monitoring System Based on SP37 Sensor, escrito por Binwen Huang [4], se puede observar cómo varía la trama de datos del sistema TPMS basado en el sensor SP37.

Figura 4.2: Trama TPMS basado en el sensor SP37

Pressure	Temperature	Voltage	Acceleration	Synchronization code	Tire ID	Status bit	Alarm bit	Correction value	CRC8
8 bit	8 bit	8 bit	8 bit	16 bit	24 bit	8 bit	8 bit	8 bit	8 bit

El *hardware* utilizado por los sensores de los dispositivos TPMS también varía en función del fabricante. En el artículo sobre el sensor SP37 se especifican las unidades de medida, el rango de medición y el tiempo de medida. Conocer los detalles sobre el sistema de medición utilizado por los sensores es imprescindible para la construcción de la trama.

Figura 4.3: Capacidad de medición del sensor SP37

	Pressure	Temperature	Acceleration	Voltage
Meassuring range	100~450 KPa	-40~125 ºC	-12~115 g	1,8~3,6 V
Meassuring accuracy	1,37 Kpa	1 ºC	0,5 g	0,0184 V
Meassuring time	6 ms	1,5 ms	6 ms	17 ms

En este estudio se analizarán dos de los dispositivos soportados por el *software* RTL_433, construyendo el formato de la trama correspondiente de los sistemas TPMS diseñados por las marcas Citroën y Toyota.

4.2.1. Citroën

Este dispositivo se caracteriza por utilizar una modulación FSK (1.7) con una codificación Manchester. El formato de la trama podemos encontrarlo en el repositorio oficial del programa RTL_433:

- Preamble:

  Se utiliza para indicar el inicio de la comunicación al receptor y para sincronizar los relojes del emisor y el receptor. Es necesario el envío de 16 bits con la secuencia (0,1).

  En este caso, para que el receptor acepte la trama el preámbulo debe contener la siguiente secuencia de símbolos:

  $$\text{Preamble } = [0101\ 0101\ 0101\ 0101\ 0101\ 0101\ 0101\ 0110]$$

- State:

  Para informar sobre el estado es necesario el envío de 8 bits.

- ID:

  Para que el sistema central o ECU reciba la información adecuadamente cada rueda debe diferenciarse mediante un identificador único. Son necesarios 32 bits.

- Flags:

  Para informar al receptor son necesarios 4 bits.

- Repeat:

  Es un contador de repeticiones con la función de mantener informado al receptor sobre cuántas veces se ha enviado la trama. Son necesarios 4 bits.

- Pressure:

  La presión en el caso de este dispositivo se expresa en kPa (Kilopascales) con un factor de escala de 1.364 pasos. Para poder enviar esta información serán necesarios 8 bits y primeramente se deberá realizar la siguiente operación:

$$\text{Pressure to codify} = \frac{\text{Real pressure}}{1{,}364}$$

- Temperature:

  La temperatura en este dispositivo se encuentra desplazada en un exceso de -50 grados Celsius. Este desplazamiento es un factor de escala que se utiliza para ajustar los valores de la temperatura a los valores mas típicos y para poder representar valores negativos. Para representar el valor deseado deberemos aumentar en cincuenta la temperatura y serán necesarios 8 bits para el envío.

$$\text{Temperature to codify} = \text{Real Temperature} + 50$$

- Battery:

  En este caso en particular, el dispositivo también informa acerca del estado de la batería. Esta información es útil, ya que uno de los inconvenientes de estos dispositivos es la durabilidad de la pila interna. Para el envío de esta información son necesarios 8 bits.

- Checksum:

  Sirve para el tratamiento de errores durante el envío. Para calcular esta secuencia de comprobación se separa la trama en grupos de 8 bits y se calcula la operación XOR entre cada uno de ellos. Como resultado se obtienen los 8 bits de comprobación.

- End of frame:

  Sirve para indicar al receptor el fin del envío de la información. Es necesario el envío de la siguiente secuencia de símbolos:

$$\text{End of frame } = [0111\ 1110]$$

4.2.2. Toyota

Este dispositivo utiliza una modulación FSK (1.7) con una codificación Manchester Diferencial. El formato de la trama podemos encontrarlo igual que en el caso anterior en el repositorio de Benjamin Larsson [5]:

- Preamble:

  En este caso el dispositivo Toyota utiliza 14 bits como preámbulo. Esta secuencia debe contener la siguiente información:

$$\text{Preamble } = [01\ 0101\ 0100\ 1111]$$

- ID:

  Para identificar los sensores de manera única son necesarios 32 bits.

- Status:

  Después de enviar el ID del dispositivo se envía parte del estado. El estado está compuesto por 8 bits y solo se enviará el primer bit de la cadena.

- Pressure:

  La presión se expresa como un cuarto del valor real desplazado en un valor 7. Esta información requiere 8 bits y es necesario realizar la siguiente operación:

$$\text{Pressure to codify} = (\text{Real pressure} + 7) * 4$$

- Temperature:

  La temperatura se encuentra desplazada en un exceso de -40 grados Celsius. Para el envío de esta información son necesarios 8 bits y realizar la siguiente operación:

$$\text{Temperature to codify} = \text{Real temperature} + 40$$

- Status_2:

  Después del envío de la temperatura se envía la información restante del estado. Los 7 últimos bits de los 8 correspondientes.

- Pressure_2:

  Después de enviar la totalidad del estado se envía la presión en formato invertido. Son necesarios 8 bits y es un medio más para la comprobación de errores.

- Checksum:

  Para la comprobación de errores se utiliza un CRC de 8 bits. Para implementar el código que realiza esta operación utilizaremos como base una vez más el repositorio de Larsson [5].

- End of frame:

  Para indicar el fin de la trama se empaquetan 3 bits. La codificación Manchester Diferencial retorna como resultado la trama codificada y el bit resultado[1]. La negación del bit resultado será la información que compondrá el final de la trama.

[1]Este bit se utiliza para calcular las transiciones correspondientes a Manchester Diferencial y se actualiza almacenando el final de dicha transición.

$$\text{End of frame} = [000] \text{ if result bit} = 1$$

$$\text{End of frame} = [111] \text{ if result bit} = 0$$

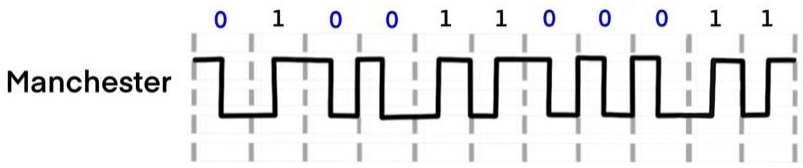
4.3. Codificaciones

Como se ha descrito en el apartado 1.1 existen varios tipos de codificación. Habitualmente en los dispositivos TPMS las codificaciones más utilizadas son Manchester o Manchester Diferencial, provocando como consecuencia un aumento de longitud de la trama original hasta duplicarla, pero garantizando la sincronía de bit.

4.3.1. Manchester

La codificación Manchester es sensible a los flancos producidos por los cambios entre símbolos, utilizando dos símbolos para definir un flanco de subida (0,1) o de bajada (1,0).

Figura 4.4: Ejemplo de codificación Manchester

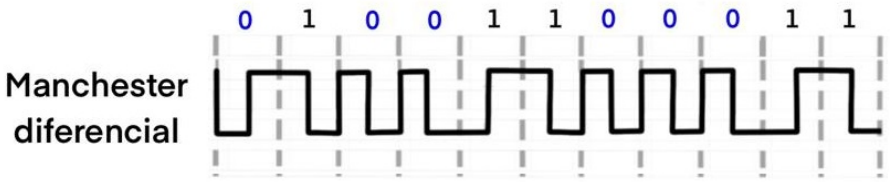


4.3.2. Manchester Diferencial

La codificación Manchester Diferencial es sensible a la presencia o ausencia de transiciones. Para implementar esta codificación se recorre la trama calculando las transiciones mediante el uso de un bit resultado inicializado a uno. Teniendo en cuenta la mitad de la

transición y el inicio de la siguiente, las posibles transiciones pueden expresarse como (0,0), (0,1), (1,0) o (1,1).

Figura 4.5: Ejemplo de codificación Manchester Diferencial



4.4. Diagrama de bloques de GNU-Radio

En este apartado se procederá a utilizar Gnu-Radio para obtener la modulación de los datos digitales para cada trama TPMS, lo que generará como resultado la señal analógica correspondiente.

En el apartado 4.2 se ha podido observar cómo se debe construir la trama adecuada para los dispositivos que se utilizarán de ejemplo. Una vez construida la trama se debe proceder a su codificación como en el apartado 4.3.

Una vez concluida la codificación que utiliza el dispositivo TPMS, la siguiente cuestión a tratar será la modulación que utilizará para transmitir la señal. Los diferentes tipos de modulación son: FSK (figura 1.7), ASK (figura 1.3), OOK (figura 1.4) y PSK (figura 1.5). Las modulaciones más utilizadas por los fabricantes de los dispositivos TPMS son ASK, OOK y FSK.

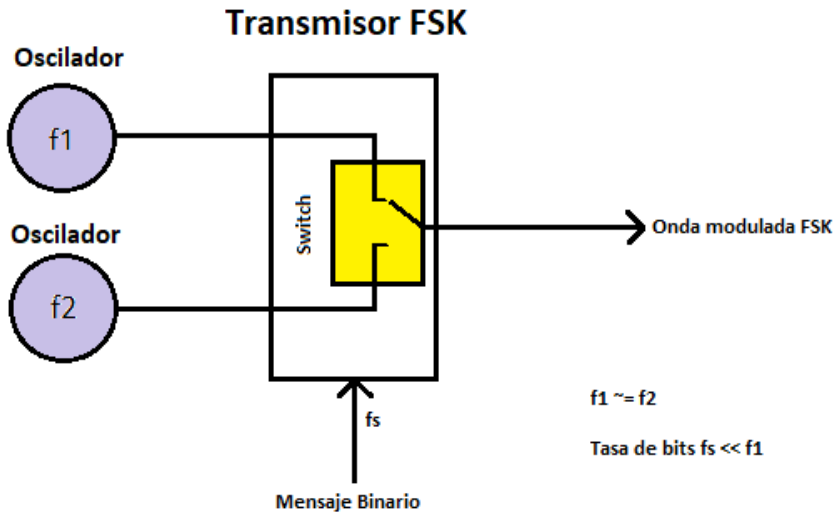
La codificación en el caso de Citroën es Manchester y el caso de Toyota es Manchester Diferencial. Como se ha explicado en capítulos anteriores la señal debe generarse utilizando una modulación específica, en este caso ambos dispositivos utilizan la modulación FSK.

Existen varios medios para generar esta señal como podría ser Matlab o Gnu-Radio, y

se han realizado pruebas para ambas aplicaciones, pero mediante el uso de Matlab no se ha conseguido el resultado esperado. Sin embargo, Gnu-Radio es una aplicación específica para la generación y el análisis de señales, que dota al usuario de un amplio conjunto de herramientas que permiten la obtención de la señal modulada.

La modulación es una etapa compleja, pero de concepto simple. En el caso de BFSK (Binary FSK) el concepto podría reflejarse como en la figura 4.6.

Figura 4.6: Diagrama de bloques FSK



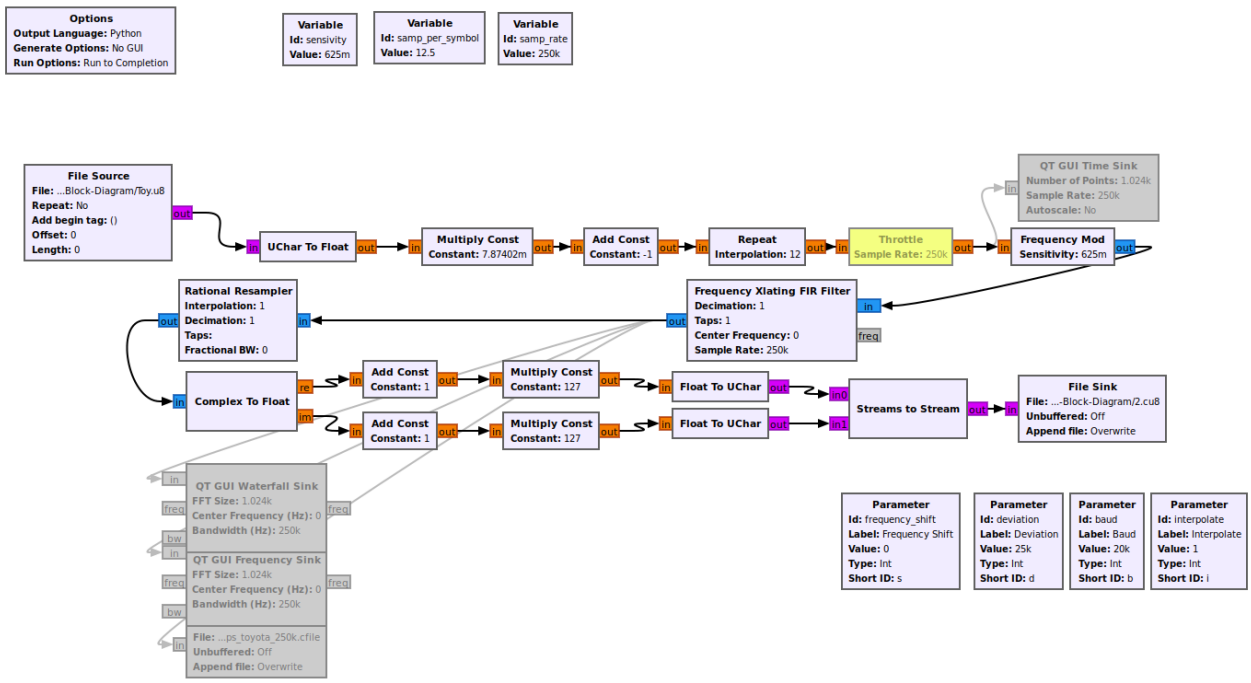
Como podemos observar el proceso de modulación estaría compuesto por tantos osciladores como número de símbolos necesitemos para codificar la información. En este caso son necesarios dos osciladores [f1, f2] correspondientes a los símbolos [0, 1] respectivamente.

Estos osciladores son conectados a un *switch* encargado de activar una entrada u otra en función de la cadena de símbolos que se desee transmitir. De esta forma se consigue la onda modulada en FSK cuyo aspecto podemos comprobar en la figura 1.7.

En Gnu-Radio este objetivo se puede conseguir mediante el diagrama de bloques repre-

sentado en la figura 4.7. Este diagrama de bloques ha sido construido por Cyril [2]. Dentro de este diagrama de bloques podemos observar tres etapas: lectura del archivo binario que almacena la trama codificada, modulación digital de los datos y escritura de la señal modulada.

Figura 4.7: Diagrama de bloques BFSK en Gnu-Radio



- Lectura del archivo binario

  Mediante el módulo `File Source` se observa cómo se puede realizar la lectura de un archivo binario con la señal codificada.

  Posteriormente es necesario preparar los datos leídos para poder proceder a su modulación. Este proceso se lleva a cabo mediante los módulos `Uchar To Float`, `Multiply Const`, `Add Const` y `Repeat Interpolation`.

Por último, el módulo `Throttle` aplica la frecuencia de muestreo que llevará la señal, siendo su valor de 250kHz.

- Modulación

  El módulo `Frequency Mod` consigue modular la señal en FSK, obteniendo como resultado la señal en un amplio rango de bandas de frecuencia que será necesario filtrar.

  Para filtrar la señal y seleccionar las bandas de frecuencia correspondientes a 433MHz se utiliza el módulo `Frequency Xlating FIR Filter`, lo que permite obtener como resultado una señal compleja de tipo IQ.

- Escritura de la señal

  Con el objetivo de posibilitar la escritura en un archivo de tipo `cu8` es necesario formatear los datos obtenidos tras la modulación. Para la escritura de este tipo de archivo se utilizará el módulo `File Sink`.

En resumen, mediante un archivo de formato binario con la secuencia bits codificada se consigue modular la señal con una frecuencia de muestreo (Sample Rate) de 250kHz. Se genera de esta forma una señal compleja que corresponde con la señal que se desea emitir. Esta señal se puede almacenar en un archivo o bien transmitirla mediante cualquier dispositivo específicamente preparado para ello, por ejemplo, HackRf One [7].

Capítulo 5

Señales generadas

Las pruebas físicas de emisión no han podido llevarse a cabo debido a la pandemia mundial actual, por lo que en este capítulo se explicará como comprobar la viabilidad de una señal generada sin disponer de un módulo que pueda emitirla. Adicionalmente, se mostrarán las distintas señales generadas para los dispositivos TPMS correspondientes a las marcas Toyota y Citroën, para demostrar cómo se puede generar una señal con los datos no alterados o alterados, pretendiendo simular un ciberataque.

5.1. Tratamiento de la Señal

En el capítulo 4.3 se ha explicado cómo, mediante la construcción de la trama codificada a través de diferentes técnicas y Gnu-Radio se puede generar un archivo, que almacene la información relativa a la señal.

El siguiente paso consiste en comprobar la validez de la señal para lo cual se ha utilizado el *software* RTL_433. Este programa cuenta con la opción -r que permite leer distintos tipos de archivo, entre estos el que se ha generado mediante el diagrama de bloques de Gnu-Radio que es de tipo `cu8`. De esta forma se obtiene la señal demodulada y se consigue visualizar

la información por consola en formato decimal.

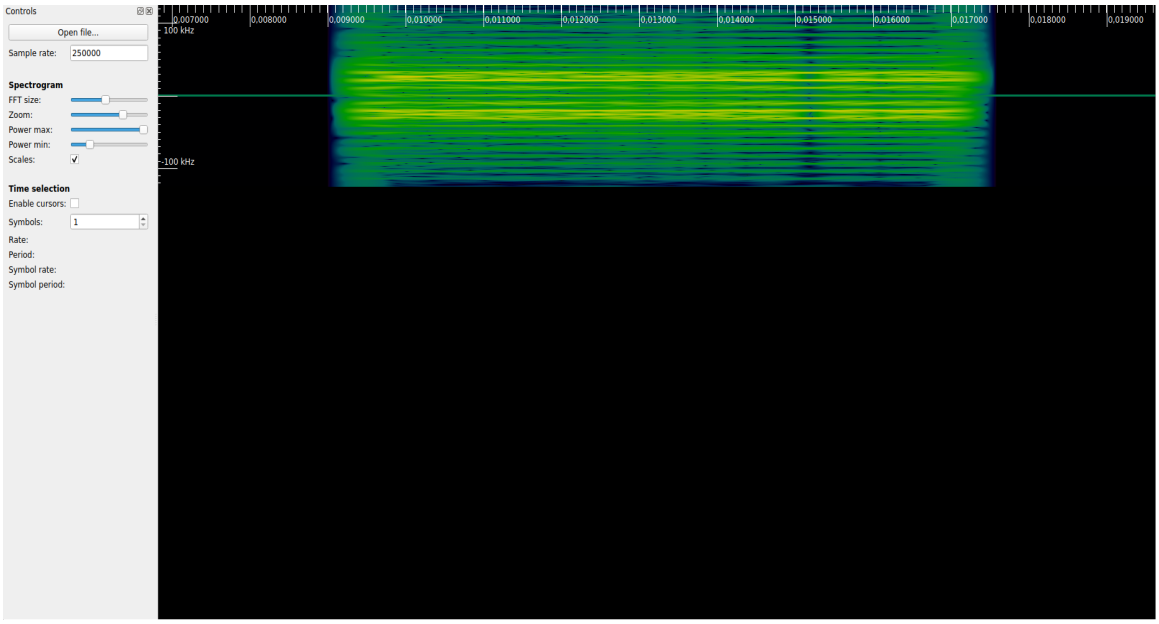
El archivo generado mediante Gnu-Radio todavía no es apto para ser leído mediante RTL_433. Esto se debe a que la señal que se genera es muy rápida y el *software* necesita de información previa sobre como realizar el muestreo para poder demodular/descodificar la señal.

Para solucionar este problema hay que dotar a la señal de silencio tanto en la parte inicial como en la parte final. Para añadir dicho silencio se utilizará SoX [1].

SoX es una utilidad que permite leer y escribir archivos de audio en los formatos más utilizados, además permite aplicar efectos de todo tipo a la señal. En este caso se busca añadir silencio a la señal con una frecuencia de muestreo de 250kHz.

Después de añadir silencio a la señal Inspectrum debería mostrarnos como resultado un espectro de frecuencia parecido al de la figura 5.1.

Figura 5.1: Espectro de la señal después de añadir silencio, visualizada con Inspectrum



Al llevar a cabo esta modificación será factible emitir nuestra señal o archivo mediante

el uso de Gnu-Radio y HackRf One.

HackRF One es un transceptor semidúplex SDR fabricado por la empresa Great Scott Gadgets y creado por Michael Ossmann et al [7]. Este dispositivo es capaz de alcanzar frecuencias de 1MHz a 6GHz, por lo que permite emitir la señal generada por Gnu-Radio.

Este transceptor, dependiendo de la banda, transmite con una potencia de 1mW a 30mW. El dispositivo dispone de conector de antena SMA, puertos CLKIN/CLKOUT SMA y un puerto USB. Gnu-Radio proporciona servicios para integrar este transceptor, por lo que a través del propio diagrama de bloques se puede añadir el módulo correspondiente a HackRf One.

Este transmisor tiene un precio muy elevado, y supera el presupuesto de este proyecto. Existen otras opciones mas económicas para el envío de la señal, como es el uso de una Raspberry pi y un modulo de emisión RF. Sin embargo, no ha sido posible realizar las pruebas necesarias de emisión al no poder adquirir estos dispositivos debido a la actual crisis sanitaria. Pese a este inconveniente se podrá demostrar la viabilidad de la señal generada por Gnu-Radio mediante el programa RTL_433, ya que este es capaz de capturar las señales de muchos de los dispositivos TPMS oficiales.

Si el *software* RTL_433 es capaz de capturar la señal y proceder a su demodulación de manera exitosa, se puede afirmar que la señal cumple con los requisitos necesarios para su emisión y que a su vez es adecuada para la recepción de la ECU del vehículo.

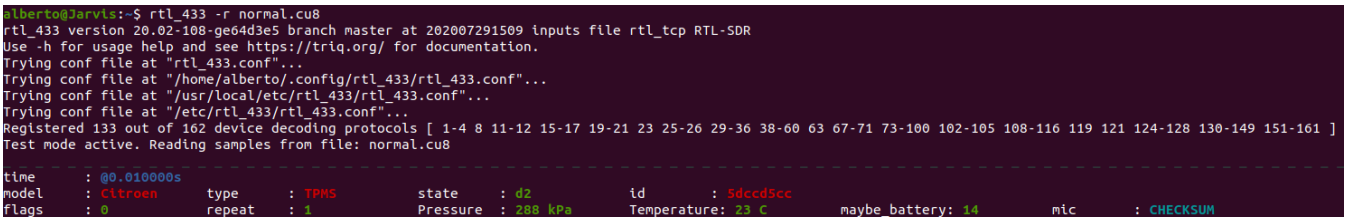
5.1.1. Dispositivo TPMS Citroën

En la sección 4.2.1 se ha podido observar el formato de la trama TPMS de este dispositivo. La señal ha sido generada mediante la codificación Manchester y la modulación FSK descritas en los apartados 4.4 y 4.7 respectivamente.

Después de añadir silencio a la señal con SoX y mediante el uso del protocolo RTL_433 se obtiene la demodulación de las tramas que se enumeran a continuación.

- Trama habitual de un vehículo con neumáticos en buen estado (figura 5.2):

Figura 5.2: Demodulación de señal de un dispositivo TPMS Citroën/ RTL_433

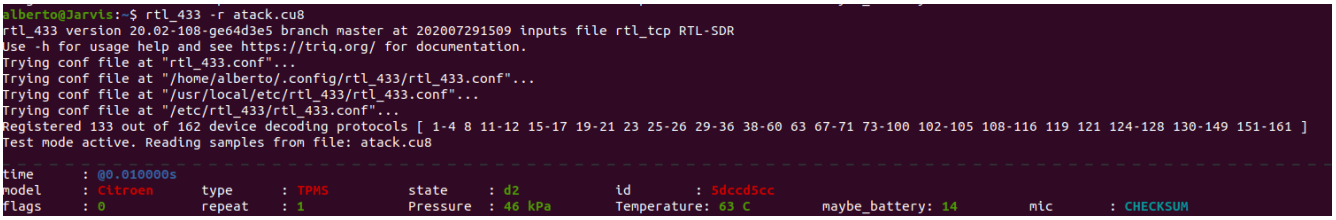


La trama de la figura 5.2 representa un neumático cuyo id tiene un valor en hexadecimal de 5dccd5cc, una presión de 288kPa (unas 2,8 atm) y una temperatura de 23ºC.

En este caso el sistema central del vehículo no interpretará ninguna amenaza, esto se debe a que la presión y la temperatura de las ruedas se encuentran en el rango de normalidad establecido por el fabricante.

- Trama modificada con el objetivo de simular un ciberataque (figura 5.3):

Figura 5.3: Demodulación de señal alterada sobre un dispositivo TPMS Citroën/ RTL_433



La trama de la figura 5.3 representa un neumático cuyo id tiene un valor en hexadecimal de 5dccd5cc, una presión de 46kPa (0,45 atm) y una temperatura de 63ºC.

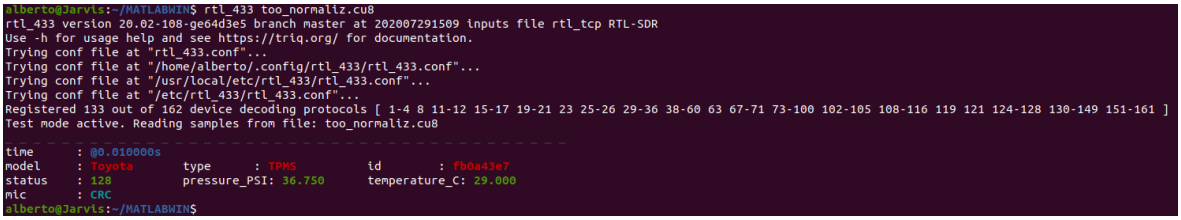
En este caso el sistema central del vehículo identifica que la presión y la temperatura de las ruedas se encuentran fuera de los valores de normalidad, por lo que procede a emitir una alerta.

5.1.2. Dispositivo TPMS Toyota:

En este caso la señal ha sido generada mediante la codificación Manchester diferencial y la modulación FSK descritas en los apartados 4.5 y 4.7 respectivamente. Como resultado se obtienen tramas de ejemplo como las enumeradas a continuación.

- Trama habitual de un vehículo con neumáticos en buen estado (figura 5.4):

Figura 5.4: Demodulación de señal de un dispositivo TPMS Toyota/ RTL_433



En la figura 5.4 se observan los valores normales de un neumático cuyo id tiene un valor en hexadecimal de fb0a43e7, una presión de 36,750psi (libras por pulgada cuadrada que equivalen a 2.5 atm) y una temperatura de 29ºC. El sistema de alerta de la ECU no se activa.

- Trama modificada con el objetivo de simular un ciberataque (figura 5.5):

Figura 5.5: Demodulación de señal alterada sobre un dispositivo TPMS Toyota/ RTL_433

La trama que se observa en la figura 5.5 se ha construido con el objetivo de simular un pinchazo. El neumático tiene un valor hexadecimal de fb0a43e7, una presión de 3,750psi (0,25 atm) y una temperatura de 69ºC, lo que provoca la alerta del sistema central (ECU).

Capítulo 6

Análisis de vulnerabilidades y conclusiones

En este capítulo se llevará a cabo el análisis de la complejidad de realizar un ciberataque por vía radioeléctrica, enumerando los posibles ataques que se pueden llevar a cabo, así como sus inconvenientes y soluciones. Finalmente, el capítulo concluirá con un estudio de riesgos de los posibles ataques y se proporcionará el resumen de costes para poder llevar a cabo este proyecto.

6.1. Recepción de señales TPMS

Como se ha podido ver durante el desarrollo de este proyecto, la recepción de señales TPMS ha sido el proceso más sencillo de todos los que se han llevado a cabo.

La señal de radio de los dispositivos TPMS se emite en abierto y sin cifrado, esto ha facilitado a desarrolladores de software mediante ingeniería inversa documentar el formato de la trama y las características de la señal de estos dispositivos. Un ejemplo de este trabajo se ha podido ver durante el desarrollo de este proyecto, para lo cual se ha usado para la recepción, un dispositivo RTL_SDR y para la demodulación, el protocolo RTL_433 [5].

6.2. Ciberataques: suplantación y tracking de vehículos

La identificación de un vehículo no solo puede llevarse a cabo mediante su matrícula o número de bastidor, sino que también puede identificarse a través de los diferentes dispositivos electrónicos presentes en el vehículo. Dentro de estos dispositivos se incluyen los sistemas TPMS, que como se ha visto en la sección 4.2 tienen asociado un identificador único de 32 bits.

Si se tiene en cuenta que la señal transmitida por estos dispositivos puede ser captada mediante el uso de un receptor SDR y el uso de software libre, la posibilidad de llevar a cabo el rastreo de un vehículo sería una tarea tanto económica como sencilla.

Una alternativa al rastreo de vehículos es la suplantación. Mediante el uso de equipos de radio, que son capaces de transmitir diferentes señales de radiofrecuencia, se pueden llevar a cabo diferentes ataques de repetición a partir de una señal previamente emitida. En este proyecto se muestra cómo alterar los datos emitidos y provocar de esta forma la confusión del sistema central o ECU.

Normalmente confundir a la ECU solo origina una alerta en forma de piloto de luz en el panel de control. Pero hay que tener en cuenta que el comportamiento puede verse afectado si la ECU interactúa con otros sistemas incorporados en el vehículo.

6.3. Medios de seguridad contra estos ataques

Aplicar los diferentes mecanismos de seguridad sobre estos dispositivos no supone una gran complejidad a nivel técnico. Sin embargo, la dificultad reside en el volumen de dispositivos en uso. Cada vehículo debe tener instalado este dispositivo por obligación y con las especificaciones actuales no dispondría del nivel de seguridad necesario para evitar los

ciberataques expuestos anteriormente.

Actualmente la comunicación entre el sistema TPMS y la ECU es unidireccional, siendo la ECU el receptor y el sistema TPMS el emisor. Los medios de seguridad que se podrían aplicar sobre estos dispositivos pasarían por poder emplear técnicas de cifrado y autenticación de la comunicación entre la ECU y el sistema TPMS. Igualmente, es necesario facilitar el emparejamiento en caso de sustituir el sensor.

6.4. Conclusiones

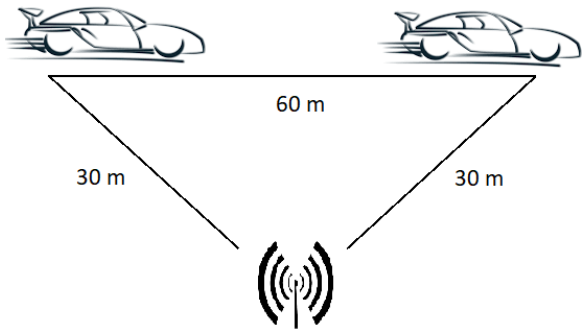
El sistema TPMS es vulnerable a diferentes ataques debido a que la comunicación es abierta y no lleva implementado ningún tipo de cifrado o autenticación. Sin embargo, llevar a cabo estos ataques es algo complejo.

Durante el estudio se ha podido observar que los dispositivos transmiten la señal en intervalos de tiempo de [30-60] segundos dependiendo del modelo. Si se quisiese llevar a cabo un ataque de seguimiento de vehículos utilizando una antena con un alcance de recepción de 30 metros en cada dirección, y si un vehículo mantuviese una velocidad constante de 50 Km/h, al encontrarnos en un estadio de MRU (Movimiento Rectilíneo Uniforme), como se puede observar en la figura 6.1, sería posible calcular el tiempo de emisión del sistema TPMS en el rango de los 60 metros de actuación de la antena:

$$\text{tiempo} = \frac{\text{espacio}}{\text{velocidad}} = \frac{30 * 2 \text{ m}}{13{,}88 \text{ m/s}} = 4{,}32 \text{ segundos}$$

Lo que quiere decir que de encontrarnos en un lugar estático para recibir la señal, solo dispondremos de 4,32 segundos para poder recibirla. Además, es posible la no recepción debido a que el sistema TPMS podría encontrarse en un periodo de no emisión.

Figura 6.1: MRU en función de una antena con un rango de actuacion de 30 metros



Pese a esto, el seguimiento de vehículos puede llevarse a cabo. Para lograr una mayor efectividad de este ciberataque se podría recurrir a alternativas como utilizar una antena con mayor alcance si la recepción de la señal se sigue realizando desde un punto estático. Otro escenario posible sería el uso de un módulo receptor que se mantenga en movimiento, ya sea en autovía o carretera, siempre que permanezca a una distancia máxima igual al rango de recepción de la antena utilizada. Con cualquiera de estas dos soluciones se podrá permanecer más tiempo en el radio de acción.

El ataque por suplantación tiene un comportamiento similar al anterior, si se emite una señal con los datos alterados, el conductor al comprobar el estado de los neumáticos podría entender que, por ejemplo, se trata de un error provocado por el sistema electrónico del vehículo. Además, si el punto de emisión se encuentra en un lugar estático, al conductor le bastaría con alejarse del punto de emisión para comenzar a recibir la señal real. Las alternativas para hacer más consistente el ataque pasan, al igual que en el caso del *tracking* de vehículos, por dotar al emisor de la señal de una antena con mayores características o cambiar a un escenario donde dicho emisor se encuentre en movimiento.

Por lo que se podría concluir que el sistema TPMS es vulnerable, siendo susceptible a diferentes ciberataques. Sin embargo, la gravedad de estos ciberataques es de carácter leve a nivel de seguridad vial, siempre y cuando la ECU del vehículo no tenga comportamientos críticos ante las señales provenientes del sistema TPMS.

6.5. Resumen de costes del Proyecto

- Andoer® Mini USB Digital Portátil 2.0 Stick.
  - 15,84 €
- Fydun TPMS Sistema de Monitoreo Control de Presión de Neumáticos [1].
  - 16.99 €
- Software Gnu-Radio.
- Software RTL_433.
- Sofware Inspectrum.
- Gqrx SDR.

Bibliografía

[1] SoX - sound eXchange | documentation. URL: http://sox.sourceforge.net/Docs/Documentation.

[2] Cyril cdeletre. TXTPMS. URL: https://github.com/cdeletre/txtpms/tree/master/modulations.

[3] Eric Fly, Steve Markgraf, Dimitri Stolnikov, and Hoernchen. Desarrolladores RTL-SDR. URL: https://osmocom.org/projects/rtl-sdr/wiki/Rtl-sdr#history_and_discovery_of_rtlsdr.

[4] Binwen Huang. Design of direct-type tire-pressure monitoring system based on sp37 sensor. *Sensors & Transducers*, 160(12):74, 2013.

[5] Benjamin Larsson. RTL_433. URL: https://github.com/merbanan/rtl_433/tree/master/src/devices.

[6] Osmocom. Osmocom. URL: https://osmocom.org/.

[7] Michael Ossmann, Taylor Streetman, Elizabeth Hendrex, Lisa Partington, Jacob Graves, Kate Temkin, and Mikaela Szekely. HackRf one. URL: https://greatscottgadgets.com/.

[8] Realtek. Driving IC innovation. URL: https://www.realtek.com/en/.

[9] Realtek. Realtek RTL2832u. URL: https://www.realtek.com/en/products/communications-network-ics/item/rtl2832u.

[10] Mike Walters. Inspectrum. URL: https://github.com/miek/inspectrum.

Apéndice A

Enlace al código

A continuación se proporciona un enlace al codigo del proyecto. https://github.com/alberc01/VULNERABILITIES-IN-THE-TPMS-PROTOCOL